

Incident response guide

Introduction

This document provides guidance for GI staff receiving incident notifications, specifically around how to initially respond, and should be used together with GI-TOC's Incident Reporting Procedure, Incident Report Form and Critical Incident Management Procedure.

Response process

GI staff receiving verbal incident reports should follow the four-step process detailed below.



Step 1 - Establish comms & emerging facts

As soon as you receive an incident notification **quickly establish communication lines**, as follows:

- **WHO** is the affected person(s)?
- **WHERE** did the incident take place and **WHERE** is the person notifying you?
- **HOW** can you contact them, ideally using end-to-end encryption? Request at least two different forms of contact.
- **WHO** is their emergency contact and **WHAT** are their contact details? This is a person you can contact if you fail to make future contact with the affected person(s).

Next **establish the emerging facts** around the incident, including:

- **WHO** has been involved and **WHERE** did the incident occur?
- **WHAT** has happened?
- **WHAT** actions have been taken so far and **WHAT** actions are going to be taken by the affected person(s)?
- **WHAT** further assistance is required?

Step 2- Ensure immediate safety

Based on the information received above, consider and agree what **immediate actions** should be implemented to ensure the affected person(s) safety. Remember, these actions should focus on reducing **immediate threats to life and safety**. The correct actions will depend on the incident and the context of the country. However, some examples include:

- Immediately cease all movements and shelter-in-place.
- Immediately leave the area for a safer location.
- Apply first aid, contact emergency services, or visit the nearest medical facility.
- Call law enforcement or other incident responders.

Step 3- Determine if it is a Limited or Critical incident

Next, together with the person notifying you of the incident, **determine if the incident is a Critical incident or Limited incident** as this will indicate who you inform and the next actions that should be implemented. To support your determination, assess whether any of the following have occurred:

Have any of the following occurred?

- Critical harm, including death, threat to life or personal safety, sexual harassment or violence, major injury, kidnap, detention, harm to mental health, or other serious impacts.
- Major operational disruption to GI-TOC, our partners, fellows or grantees.
- Major loss of assets or finance.
- Loss or breach of data / information.
- Misinformation / disinformation incidents.
- Significant challenge to GI-TOC's integrity, reputation and mission.
- Regulatory investigation.
- Legal action against GI-TOC.
- The affected person(s) requested the Critical Incident Management Team to be activated.

Yes	➔	Critical Incident	➔	The relevant manager / project manager and the Director or Deputy Director	➔	Critical Incident Management Team
No	➔	Limited Incident	➔	The relevant manager / project manager	➔	Move to step four (below)

- If the incident is a **Critical Incident**, inform the Director or Deputy Director who will activate the Critical Incident Management Team and implement relevant immediate responses.
- If the incident is a **Limited Incident**, inform the relevant manager / project manager and move to step four, below.

Step 4 - Implement immediate responses

Finally, together with the person notifying you of the incident or the affected person(s), agree and **implement immediate responses**. These responses go beyond immediate safety and focus on developing a support network and providing continued risk reduction measures. Remember, the exact responses depend on the incident and the context of the country.

1. **Develop and agree on a set of immediate responses** for the affected person(s) to implement, identifying areas where they potentially need support, e.g., funding, legal representation, physical security, digital security, wellbeing and resilience, etc.
2. **Contact potential responders**, including insurers, grantees, partners, lawyers, governments, [Open Briefing](#), etc., to assess their capacity to respond and to provide support targeted at reducing risk exposure.
3. **Agree regular check-ins** with the affected persons. At each check in, ensure that you discuss any new incidents, escalations / changes in the context, changes to the affected person(s) movements and activities, updates on mitigation, new areas of support requirements.
4. Complete an **incident report form** and continue to monitor the case.